北京依众公益基金会
信息安全工作管理制度

第一章　总则

第一条　为贯彻国家对信息安全的规定和要求，加强信息安全规范建设、建立持续改进的信息安全管理体系、实施监督检查、降低企业面临的信息安全风险、保障北京依众公益基金会（以下简称“依众基金会”）业务正常有序的运作，特制定本制度。

第二条　本制度根据、《GB/T20269-2006 信息安全技术信息系统安全管理要求》、《GB/T22239-2008 信息安全技术信息系统安全等级保护基本要求》等有关法律、标准、政策、管理规范而制定。

第三条　本制度适用于北京依众公益基金会。

第二章　方针、目标、原则

第四条　依众基金会信息系统安全坚持“适度防护、预防为主，管理和技术并重，综合防范”的总体方针，实现信息系统安全可控、能控、在控。依照“分区、分级、分域”总体安全防护制度，执行信息系统安全等级保护制度。

第五条　信息系统安全总体目标是确保信息系统持续、稳定、可靠运行和确保信息内容的机密性、完整性、可用性，防止因信息系统本身故障导致信息系统不能正常使用和系统崩溃，抵御黑客、病毒、恶意代码等对信息系统发起的各类攻击和破坏，防止信息内容及数据丢失和失密，防止有害信息在网上传播，防止对外服务中断和由此造成的系统运行事故。

第六条　信息安全工作的总体原则：

（一） 依法管理原则

信息安全管理工作主要体现为管理行为，应保证信息系统安全管理主体合法、管理行为合法、管理内容合法、管理程序合法。对安全事件的处理，应由授权者适时发布准确一致的有关信息，避免带来不良的社会影响。

（二） 管理与技术并重原则

坚持积极防御和综合防范，全面提高信息系统安全防护能力，立足国情，采用管理与技术相结合，管理科学性和技术前瞻性结合的方法，保障信息系统的安全性达到所要求的目标。

（三） 自保护和国家监管结合原则

对信息系统安全实行自保护和国家保护相结合。对自己的信息系统安全保护负责，政府相关部门有责任对信息系统的安全进行指导、监督和检查，形成自管、自查、自评和国家监管相结合的管理模式，提高信息系统的安全保护。

（四） 基于安全需求原则

根据信息系统担负的使命，积累的信息资产的重要性，可能受到的威胁及面临的风险分析安全需求，按照信息系统等级保护要求确定相应的信息系统安全保护等级，遵从相应等级的规范要求，从全局上恰当地平衡安全投入与效果。

（五） 主要领导负责原则

主要领导应确立其组织统一的信息安全保障的宗旨和政策，负责提高员工的安全意识，组织有效安全保障队伍，调动并优化配置必要的资源，协调安全管理工作与各部门工作的关系，并确保其落实、有效。

（六） 全员参与原则

信息系统所有相关人员应普遍参与信息系统的安全管理，并与相关方面协同、协调，共同保障信息系统安全。

（七） 系统方法原则

识别和理解信息安全保障相互关联的层面和过程，采用管理和技术结合的方法，提高实现安全保障的目标的有效性和效率。

（八） 持续改进原则

安全管理是一种动态反馈过程，贯穿整个安全管理的生存周期，随着安全需求和系统脆弱性的时空分布变化，威胁程度的提高，系统环境的变化以及对系统安全认识的深化等，应及时地将现有的安全制度、风险接受程度和保护措施进行复查、修改、调整以至提升安全管理等级，维护和持续改进信息安全管理体系的有效性。

（九） 多级防护原则

按等级划分标准确定信息系统的安全保护等级，实行多级防护；对多

个子系统构成的大型信息系统，确定系统的基本安全保护等级，并根据实际安全需求，分别确定各子系统的安全保护等级，实行多级安全防护。

（十） 分权和授权原则

对特定职能或责任领域的管理功能实施分离、独立审计等实行分权，避免权力过分集中所带来的隐患，以减小未授权的修改或滥用系统资源的机会。任何实体（如用户、管理员、进程、应用或系统）仅享有该实体需要完成其任务所必须的权限，不应享有任何多余权限。

第七条 在规划和建设信息系统时，信息系统安全防护措施应按照“三同步”原则，与信息系统建设同步规划、同步建设、同步投入运行。

第三章 总体安全制度

第八条 依众基金会信息系统总体安全保护制度是：信息安全保护必须符合客观存在和发展规律，其分级、分区域、分类和分阶段是做好信息安全保护的前提。

第九条 依众基金会信息系统的安全保护制度由信息安全责任人负责修订。

第十条 信息安全责任人根据信息系统的保护等级、安全保护需求和安全目标，结依众基金会自身的实际情况，依据国家有关安全法规和国家标准，授权制定信息系统的安全保护实施细则和具体管理办法；并根据环境、系统和威胁变化情况，及时调整和制定新的实施细则和具体管理办法。

第十一条 信息系统安全等级的定级决定了系统方案的设计、实施、安全措施、运行维护等信息系统建设的各个环节。信息系统定级遵循“谁建设、谁定级”的原则。

第十二条 根据信息重要程度、系统重要性和安全制度将信息系统划分为不同的安全域，针对不同的安全域确定不同的信息安全保护等级，并进行相应的保护。

第十三条 信息系统的等级保护应从物理、网络、主机、应用、数据和安全管理六个部分进行，并构成系统整体安全控制机制。

（一） 物理安全包括：周边环境、门禁检查、防火、防水、防潮、防鼠和防雷，防电磁泄露和干扰，电源备份和管理，设备的标识、使用、存放和管理等。

（二） 网络安全包括：网络的拓扑结构、网络的布线和防护、网络设备的管理和报警，网络攻击的监察和处理。

（三） 主机安全包括：主机的身份鉴别、访问控制、主机安全审计、入侵防范、主机的恶意代码防范、终端接入控制、重要服务器的监控。

（四） 应用安全包括：系统登录、权限划分与识别、数据备份与容灾处理，运行管理和访问控制，密码保护机制和信息存储管理、资源控制和代码安全。

（五） 数据安全包括：数据传输的完整性和保密性、数据存储的完整性和保密性、数据的备份和恢复。

（六） 安全管理制度是信息系统安全制度、方针性文件，规定信息安全工作的体系框架、内部审核机制、评审机制及改进机制。

（七） 安全管理机构通过构建和完善信息安全组织架构，明确不同安全组织、不同安全角色的定位、职责以及相互关系，强化信息安全的专业化管理，实现对安全风险的有效控制。

（八） 人员安全管理从人员录用、人员管理、人员考核、保密协议、培训、离岗离职等多个方面都制定相应的管理制度和规定。

（九） 系统建设管理根据系统等级、系统重要性和安全制度将信息系统划分为不同的安全域，针对不同的安全域确定不同的信息安全保护等级，并进行相应的保护。信息系统安全等级决定了系统方案的设计、实施、安全措施、运行维护等信息系统建设的各个环节。信息系统定级遵循“谁建设、谁定级”的原则。

（十） 系统运维管理对环境、资产、介质、设备进行综合监控管理，对支撑重要信息系统的资源进行监控保护。确保密码、病毒、变更等事件要求按照定义好的安全管理制度措施；建立安全管理监控中心，实现人、事件、流程、资产的综合管理。

第四章　制度的制定与发布

第十四条　秘书处负责制订信息系统安全管理制度，并以文档形式表

述，报批理事会审议发布。

第十五条 信息安全责任人负责组织制度编制、组织相关人员进行论证、监督检查和修订。

第十六条 信息系统安全管理制度应进行版本控制。

第十七条 信息安全管理制度由秘书长负责审核，按照依众基金会程序正式发布。

第五章 制度的评审和修订

第十八条 由信息安全责任人和秘书长负责文档的评审，对安全制度和制度的有效性进行程序化、周期性评审，并保留必要的评审记录和依据。

第十九条 信息安全责任人负责定期组织对安全管理制度的执行情况进行检查。

第二十条 结合国家信息安全主管部门每年定期对信息安全进行检查中发现的问题，信息安全责任人负责对信息安全管理制度进行有针对性的修订与完善。

第二十一条 当发生重大安全事故、出现新的安全漏洞以及技术基础结构发生变更时，信息安全责任人要对安全管理制度的实施细则进行修订；修订后的实施细则报综合管理部进行备案。

第二十二条 每个制度和制度文档有相应负责人或负责部门，负责对明确需要修订的文档进行维护。

第六章 信息安全岗位职责要求

第二十三条 关键事务岗位应配备多人共同管理，定期轮岗；关键岗位人员配备坚持“权限分散、不得交叉覆盖”的原则。

第二十四条 信息安全责任人应根据岗位职责，确定岗位所需要的安全技能，对所有信息安全岗位人员进行对应的安全技能培训。

第二十五条 信息安全主管的岗位职责：

（一） 组织、协调落实各项信息安全工作；

（二） 组织评审信息安全总体制度、规划方案、管理制度和技术规范；

（三） 组织评审信息安全产品技术规格和相关产品安全规格；
（四） 组织监督、检查信息安全工作的落实情况。
第二十六条 安全审计员的岗位职责：
（一） 定期审计信息安全制度执行情况，收集信息系统日志和审计记录，并提供审计报告；
（二） 制定信息安全审计的范围和日程，召开审计会议，管理具体的审计过程，分析审计结果并提出对信息安全管理体系的改进意见；
（三） 对安全管理员、系统管理员的操作行为进行监督，安全职责落实情况进行检查；
（四） 组织检查各部门信息系统安全人员及关键岗位人员的信息安全工作；
（五） 对相关人员提供审计培训；
（六） 推动信息安全方针、信息安全制度、信息安全管理制度及信息安全技术规范的实施落实。
第二十七条 安全管理员的岗位职责：
（一） 定期组织信息系统漏洞扫描和信息安全风险评估工作，形成信息系统和整体安全现状报告，并向行政部汇报；
（二） 负责制定总体网络访问控制制度和规则，并对其进行监控和审计工作，定期发布制度执行情况；
（三） 负责制定全员的安全培训计划，组织开展安全培训工作；
（四） 对系统管理员进行安全指导；
（五） 定期收集信息安全漏洞和公告信息，告知系统管理员。
第二十八条 系统管理员的安全职责：
（一） 确认和更新岗位所辖资产；
（二） 负责非涉密介质的维护、维修工作，及相关系统的建设、日常管理和运行维护等技术支持保障工作。
（三） 协助资产负责人进行资产清册更新、实物盘点、核对工作。
（四） 根据安全制度定期对系统进行自评估；
（五） 依照安全制度对系统进行安全配置和漏洞修补；
（六） 对系统进行日常安全运维管理，定期更改系统账号，并定期提交安全运行维护记录或报告；

（七） 在发生系统异常和安全事件时，应能对系统进行应急处置。

第七章 数据备份与恢复管理办法

第二十九条 目标

为了建立有效的备份及恢复机制，保障信息系统数据安全及各应用系统的正常运行。

第三十条 适用范围

本规定适用于系统范围内的数据备份管理。

第三十一条 数据备份与恢复基本要求

（一） 应有专门人员负责数据备份及恢复。

（二） 正式使用的应用系统、操作系统、数据库系统、网络系统等的业务数据和系统数据必须定期进行有效备份。

（三） 备份数据必须定期、完整、真实、准确地转储到备份介质，备份介质需要满足保存期限要求，备份介质应进行标识，备份情况应有记录。

（四） 备份管理人员应定时检查备份记录，如发现有备份任务失败的记录，及时查明原因、排除故障后备份。

（五） 应定期进行数据恢复测试，并基于测试结果改进备份方案。

（六） 备份管理人员不得泄露备份数据。

第三十二条 数据备份

（一）备份制度

1、完全备份

完全备份是将服务器上的所有数据都进行备份。该方式需要比较大的存储空间以及要花费较多的时间。但是它可较快地进行恢复。

2、增量备份

增量备份是只备份前一次备份以后的数据变化。该方式每次备份花费的时间较少，但需要较多的恢复时间。

3、差异备份

差异备份是只备份前一次完全备份以后的变动数据。该方式比完全备份所花的时间要少，而需要的恢复时间要少于增量备份。

（二） 备份任务

1、临时性任务

因系统变更等原因，服务器管理员可提出临时性备份任务，临时性任务根据备份提出人要求及时实施。

2、周期性任务

周期性任务分为每日备份一次、每周备份一次、每月备份一次及或更长周期。

（三） 备份提出与实施

1、服务器系统管理员作为服务器数据备份的提出人，确定数据备份内容、方式及备份周期，向备份管理人员提交数据备份申请。

2、桌面计算机数据由该机使用人员负责向行政部提出数据备份申请，行政部经过审核后向备份管理员提交数据备份申请。

3、备份管理人员对备份申请进行审核，制定备份方案，提交行政部主管领导审核，通过后实施。

第三十三条 数据恢复

发生系统故障或数据破坏等情况时，由备份管理员进行备份数据的恢复，服务器系统管理员迅速恢复系统，确保系统正常运行。

（一） 数据恢复测试

1、每半年进行一次备份数据恢复测试，测试应在测试环境中进行，严禁在正式使用的系统中进行恢复测试。

2、恢复测试内容包括备份数据恢复、系统恢复、故障排除等内容。如果发现不能恢复的数据，应及时查明原因，采取相应措施，确保备份数据的有效性。

3、测试结束后及时清除测试环境数据。

（二） 数据恢复提出与实施

1、系统管理员作为数据恢复的提出人，确定数据恢复要求，向备份管理人员提出数据恢复申请。

2、桌面计算机数据由使用人员向行政部提出数据恢复申请，经过审核后向备份管理员提出数据恢复申请。

3、备份管理人员负责实施数据恢复。

（三） 备份介质管理

1、备份介质要由专人负责保管工作，备份介质要严格管理、妥善保

存。

2、备份介质应在指定的场所保管，保存地点应有防火、防热、防潮、防尘、防磁等设施。

3、不再使用的备份介质应及时销毁。

第八章　外部人员信息安全的管理

第三十四条　依据《GB/T22239-2008 信息安全技术 信息系统安全等级保护基本要求》等有关法律、标准、政策、管理规范而制定。

第三十五条　本章内容适用于为依众基金会提供信息技术和相关服务的第三方公司和人员。

第三十六条　加强对外部人员访问的安全管理。应对外部人员允许访问的区域、系统、设备、信息等内容进行限制。

第三十七条　外部人员访问重要安全区，应由信息安全责任人批准后，按临时权限授权并由人员陪同，并登记备案。

第三十八条　外部人员访问办公场所，应登记备案。

第三十九条　外部人员应佩带易于识别的标志，并在访问重要场所时有专人陪同。

第四十条　外部人员如需常驻依众基金会，应由信息安全责任人审核其访问需求，进行风险分析，采取控制措施。在相应的控制措施未落实之前，外部人员不得访问依众基金会的内部网络与信息系统。

第九章　附则

第四十一条　本制度由秘书长监督实施；本制度的修订由秘书处提出修改意见，报理事会审议通过后执行。

第四十二条　本制度由北京依众公益基金会秘书处负责解释，经2023年04月24日第二届理事会第一次会议表决通过，自2023年04月24日起施行。